IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
GALVESTON DIVISION

MAGDOLINE HAMMAD
Plaintiff,

v. CIVIL ACTION NO. 4:20-cv-3142

RAMSEY HAMMAD
Defendant,

DEFENDANT RAMSEY HAMMAD'S RESPONSE TO PLAINTIFF'S AMENDED MOTION FOR PRELIMNARY INJUNCTION

Comes Now, Ramsey Hammad, hereinafter referred to as Defendant, who files this response to Plaintiff's requested preliminary injunction and would show the court as follows:

SUMMARY OF ARGUMENT

The Court should deny Plaintiff's request for injunctive relief because the Defendant's conduct is not actionable under the Electronic Communications Privacy Act (ECPA) or under the state wiretap statute because there was no "interception" as that term has been defined by the courts. As such, the Plaintiff cannot prevail on the merits of their claim as required to obtain injunctive relief. Further, Plaintiff has no claim under the Stored Communications Act because text messages and voice mails within a Plaintiff's cell phone are not contained in "electronic storage" as defined by the SCA and are thus outside the scope of the statute. Additionally, Plaintiff had provided her password to the Defendant while they have been married and that password has never changed. Plaintiff has the same password for every device and knew that Defendant knew what it was. Her children know the passwords also. Therefore, she consented to Defendant's accessing the device and had no expectation of privacy within that device.

BACKGROUND

Plaintiff and her attorney are conspiring to commit the perfect scam upon the Court. They are misleading this Court about the true nature of the text messages and why they fear it's disclosure in a courtroom. That is their true concern. It is questionable whether undersigned counsel can specifically describe the contents of the messages until there has been a ruling on whether the communications are protected by the ECPA. If the messages are protected, then counsel is restricted from using them in Court by the statute. While this response will demonstrate the messages are not protected by the act, undersigned counsel has elected not to provide them to the court or state with specificity contents of the communications until ordered by the Court or until the Court has decided if Defendant's conduct violates the ECPA. As a preliminary matter this Court should order an in-camera inspection of the text messages and voice mails so it can determine the true nature and scope of the actual dispute.

Plaintiff and Defendant have been married for 21 years and have 5 children. In late August, Defendant was surprised to learn that the Plaintiff wanted a divorce. *(Exhibit 1).* For the next couple of weeks, Defendant tried to convince the Plaintiff that they should remain married. (*Id.).* During their marriage, Plaintiff had provided Defendant her passcode to all her electronic devices. *(Id.)* The pass code was her birthday. On numerous occasions, throughout the marriage, Defendant would gain access to those devices for a variety of reasons. (*Id*.) Plaintiff was fully aware that the Defendant was accessing her devices with the password that she had given him. *(Id.*) Plaintiff had access to Defendant's passwords for email among other electronic devices. (*Id.*)

After Plaintiff disclosed her intention to file for a divorce, Defendant began to notice that the Plaintiff would disappear for lengthy time periods. (*Id.*) Defendant could not figure out where Plaintiff was or why she was never home. (*Id*.) During this period of time, Defendant was interacting with family members and friends of Plaintiff in an attempt to save the marriage. *(Id.*)

The family members told the Defendant that the Plaintiff had complained of his domineering personality. (*Id.*)

Late at night on September 7, 2020 Defendant accessed the phone using the password previously provided by Plaintiff. (*Id.*) Defendant took screen shots of text messages and retrieved voice mails. *(Id.).* Later that morning, he provided the text messages to the family members and a mutual friend that he had previously contacted so he could demonstrate that Plaintiff had been lying about why she wanted a divorce. (*Id.*)

The text messages were stored in Plaintiff's phone and had been exchanged for the prior two- day period between Plaintiff and another individual. (*Id.*) There were also voice mails left that were stored within Plaintiff's personal voice mail. *(Id.)* Importantly, Defendant did not access the text messages or the voice mails simultaneous with their transmission. (*Id.*)

Defendant confronted Plaintiff at around 2:00 AM with the messages on September 8, 2020. The Defendant, at 6:34 AM, received a threatening email with an attached letter from Hamilton Rucker that threatened him with criminal penalties to resolve a civil matter and threatened him with litigation under the ECPA. (*Exhibit 2*) Mr. Ramsey contacted undersigned counsel that morning. No further texts nor contents from the phone have been sent to other individuals after the Defendant contacted undersigned counsel.

Mr. Rucker emailed this lawsuit to Defendant on September 9, 2020 and forwarded a copy of it to the homeowner's insurance company that insures Plaintiff and Defendant's home. (*Exhibit 3*) On September 8, 2020, Mr. Rucker filed a divorce petition on behalf of Plaintiff. (*Exhibit 4*).

Undersigned Counsel contacted Mr. Rucker on September 9, 2020 and notified him that undersigned counsel was representing Defendant in the divorce action and the federal lawsuit.

(*Exhibit 5*) Counsel agreed to accept service and requested that he be notified of when the TRO would be presented to this Court. (*Exhibit 5)* On September 11, 2020, Steve Jackson, a lawyer from Montgomery County, Texas, requested that undersigned counsel agree to a substitution of counsel. (Exhibit 6) Mr. Jackson immediately filed an entry of appearance before filing the substitution. Undersigned counsel agreed to the continuance. (Exhibit 7) Mr. Rucker had a conflict of interest because he was a witness and was also Plaintiff's attorney in the divorce. He is a witness in our case as well. Lawyers are prohibited from acting as attorneys and witnesses under the Texas Rules of Disciplinary Procedure.

Plaintiff filed her original lawsuit and her requested her TRO claiming that the Defendant was employed as an IT person and had "surreptitiously and wrongfully hacked the cell phone which was password protected." *Docket No. 3*. Plaintiff filed an amended request for a TRO and changed her story. She claimed in the amended request that Defendant told her he guessed her password instead of accusing him of hacking into her cell phone. *Docket No. 8.* This Court has denied both requested TRO'S and has reserved judgment on the request for a preliminary injunction until the matter shall be heard on September 25, 2020. *Docket No. 9.*

ARGUMENT & AUTHORITIES

Title I of the Electronic Communications Privacy Act ("ECPA") protects against the unauthorized interception of wire, oral, or electronic communications. With certain exceptions enumerated in the statute, it establishes civil and criminal liability for any person who:

a. intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

b.intentionally uses, endeavors to use, or procures any other person to use or endeavor to use

any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii)such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii)such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection[.] *18 U.S.C. § 2511(1)*.

Title II of the ECPA, also known as the Stored Communications Act ("SCA"), prohibits intentional unauthorized access of stored electronic communications and transactional records.

Again, with certain enumerated exceptions, the SCA establishes civil and criminal liability for whoever:

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system. *18 U.S.C. § 2701*.

A. Defendant did not intercept communications under the ECRA has interception has been defined by courts.

Plaintiff may only succeed on her claim against Defendant if she can demonstrate Defendant intercepted her communications. All the circuit courts that have addressed the issue have agreed that the definition of "intercept" "encompasses only acquisitions contemporaneous with transmission." *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003). See *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2001); *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003); and *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107 (3rd Cir. 2003). The general reasoning behind these decisions is that based on the statutory definition and distinction between "wire communication" and "electronic communication," the latter of which conspicuously does not include electronic storage, Congress intended for electronic communication in storage to be

handled solely by the Stored Communications Act. This interpretation is reasonable and consistent with the language of the statute.

The Fifth Circuit held for an electronic communication "to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage." *Steve Jackson Games, Inc. v. U.S. Secret Serv*., 36 F.3d 457, 463 (5th Cir. 1994). "An 'interception' "require[s] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device." *United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976) Defendant retrieved text messages from a "What's App," on the cell phone that were stored for two days prior to September 8, 2020. He did not acquire them during transmission. *(Exhibit 1*). He also listed to voice mails. (*Exhibit 1*) The voice mails had simply not been deleted. *(Exhibit 1)* He cannot be held liable under the act because his transmission to Plaintiff's family members is only unlawful if he wrongfully intercepted the communication continuous with its transmission. The cases cited above demonstrate that the Defendant's actions did not comport with the statutory definition of "interception" because he did not access the communication contemporaneously with its transmission. Therefore, he is not liable for the dissemination of the communications under the act.

B. Defendant did not gain access to an electronic storage facility as the term is defined by courts.

Defendant conduct also did not violate the Stored Communications Act. For the Defendant to be liable under the SCA, he must have gained unauthorized access to a facility through which electronic communication services are provided (or the access must have exceeded the scope of authority given) and must thereby have accessed electronic communications while in storage. *Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 791 (5th Cir. 2012). In *Garcia*, the Plaintiff argued

that her personal cell phone was a "facility" in which electronic communication is kept in electronic storage in the form of text messages and pictures stored on the cell phone. *Id*. at 791.

The Fifth Circuit rejected this argument. Courts agree that a "home computer of an end user is not protected by the *SCA*." *Id.* at 793. "Information that an individual stores to his hard drive or cell phone is not in electronic storage under the statute." *Id.* at 793. "An individual's personal cell phone does not *provide* an electronic communication service just because the device *enables* use of electronic communication services, and there is no evidence here that the Defendants ever obtained any information from the cellular company or network. Accordingly, the text messages and photos stored on Garcia's phone are not in "electronic storage" as defined by the SCA and are thus outside the scope of the statute." *Id*. at 793.

The Court further analyzed the issue of what the act was intended to protect against. "The entire discussion of [the SCA] deals only with facilities operated by electronic communications services such as 'electronic bulletin boards' and 'computer mail facilit[ies],' and the risk that communications temporarily stored in these facilities could be accessed by hackers. It makes no mention of individual users' computers." *Id*. at 793

Plaintiff's text messages and voice mails stored on her phone are not in "electronic storage" as defined by the case law that interprets the act. As such, she has no claim under the SCA.

C. Plaintiff consented to the Defendant's receipt of the communications and had no reasonable expectation of privacy within her phone because she had supplied Defendant and other family members with the passwords to her device.

Courts have long held that a person cannot complain of an illegal intercept if they consent to allowing the communication to be intercepted. *United States v Bragan* 499 F.2d. 1376 (4th Circ. 1976) As stated earlier, there was no interception. However, Plaintiff consented to allowing Defendant to access her phone when she gave him her passwords. *(Exhibit 1)* As such, Plaintiff's consent makes Defendant's actions lawful.

A determination of whether someone has a legitimate expectation of privacy depends on two factors: (1) "whether the individual, by conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that he sought to preserve something as private;" and (2) "whether the individual's expectation of privacy is one that society is prepared to recognize as reasonable." *United States v. King*,227 F.3d 732, 743–44 (6th Cir.2000). The first factor is subjective and involves a question of fact; the second factor is objective and involves a question of law. *See United States v. Welliver*,976 F.2d 1148, 1151 (8th Cir.1992) Plaintiff would have no expectation of privacy in her cell phone when she had provided her passwords for her electronic devices to the Defendant. Her conduct has shown that she did not desire to preserve it as private from Defendant and their children. As such, she has no claim under the ECPA.

4. The Court should deny the injunction because Plaintiff cannot satisfy the elements necessary for the Court to grant her requested relief.

A district court may grant a preliminary injunction only if the movant establishes four requirements: First, the movant must establish a substantial likelihood of success on the merits. Second, there must be a substantial threat of irreparable injury if the injunction is not granted. Third, the threatened injury to the plaintiff must outweigh the threatened injury to the defendant. Fourth, the granting of the preliminary injunction must not disserve the public interest. *Cherokee*

Pump Equip., Inc. v. Aurora Pump, 38 F.3d 246, 249 (5th Cir. 1994) *Harris County Texas v. Carmax Auto Superstores*, 177 F.3d 306, 312 (5th Cir. 1999)

Plaintiff cannot establish a claim under the act. First, Defendant did not intercept her communications. Second, Plaintiff's communications were not in an electronic storage "facility". Therefore, she cannot sue Defendant under the electronic privacy and storage acts. The inability to litigate claims under the privacy statute means that Plaintiff does not have a substantial likelihood of success. Additionally, once the text messages are reviewed, the Court will learn it is the Defendant who has been injured far worse than the Plaintiff. Fourth, once the messages are reviewed, the Court will understand the granting of the preliminary injunction would allow a fraud to be perpetrated upon the court and would disserve the public interest. Thus, the request for preliminary injunction must be denied.

CONCLUSION

For the reasons set out above, this Court should deny Plaintiff's request for a preliminary injunction and the Court should inspect the disputed communications in camera and determine what further actions it should take.

Respectfully submitted,

/s/John LaGrappe
LAGRAPPE LAW PLLC
John LaGrappe
State Bar No. 11819580
Federal Bar No. 146186
440 Louisiana Suite 900
Houston, Texas 77002
713.236.7723
713.785.4187 facsimile
jlagrappe@yahoo.com

Notice of Electronic Filing

I, John LaGrappe, Counsel for Plaintiff, do hereby certify that I have electronically submitted for filing, a true and correct copy of the foregoing instrument in accordance with the Electronic Case Files System of the Southern District of Texas on September 18, 2020.

/s/ John LaGrappe

CERTIFICATE OF SERVICE

I, John LaGrappe, Counsel for Plaintiff, do hereby certify that a true and correct copy of the foregoing instrument has been served upon all counsel of record via the Electronic Case File System of the Southern District of Texas on September 18, 2020.

/s/ John LaGrappe